Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 20 — Issue 45 | November 5, 2020

November is Infrastructure Security Month

November is Infrastructure Security Month and now is an excellent time to focus on the vital role critical infrastructure – cyber and physical – plays in keeping the nation and our communities safe, secure and prosperous.

Cybersecurity and infrastructure security have come to the forefront as we've had to transition quickly to adjust our daily lives to remote work, distance education and telemedicine. The additions of a historic election, physical and cyber threats from foreign and domestic actors, and ongoing pandemic response complicate matters tremendously.

In recognition of this moment in history, the Cybersecurity and Infrastructure Security Agency (CISA) is promoting two sub-themes for Infrastructure Security Month 2020: In a Time of Transformation: Security and Response during a Global Pandemic and The Future of Securing Critical Infrastructure.

During this year's Infrastructure Security Month, CISA asks every organization to:

- Identify and prioritize essential workers' ability to work safely while supporting ongoing infrastructure operations across the nation.
- Bring awareness to misinformation, disinformation and conspiracies related to COVID-19, 5G, election security or other infrastructure, functions, or threats.
- Recognize the societal transformation of securing infrastructure and responding to disasters during a global pandemic.
- Understand the modernization of securing critical infrastructure as we defend today and secure tomorrow.

CISA has a number of resources and tools available on its website. Join CISA this November and take action to ensure America's critical infrastructure is safe, secure and resilient.

(Source: CISA)

Securing soft targets and crowded places

Foreign and domestic extremists and terrorists continue to focus on attacks against soft targets and crowded places: they are easy to surveil, rarely guarded or well-secured and one or a few people can easily do a lot of damage without a great amount of planning or training.

First responders, venues, business owners and the public can use CISA's collection of resources covering the many facets of this topic. Securing Soft Targets and Crowded Places offers planning and response guidance on active shooters, vehicle ramming, chemical attacks and fire as a weapon.

Procedural guides and training are available for first responders. Some topics include:

- Evacuation planning for stadiums.
- Bag check procedural guides.

Highlights

November is Infrastructure Security Month

Securing soft targets and crowded places

Maximizing FEMA COVID-19 Funding and Reimbursements

Webinar: NG911 Roadmap Community Progress & Virtual Learning Tips

Cyber Threats

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC).

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.

Subscribe here

- Challenges of drone attacks.
- Suspicious activity identification, reporting and insider threats.
- Identifying, preventing and responding to bombs and explosives.

See the CISA webpage for a full list of available resources and links to other agencies.

(Source: CISA)

Maximizing FEMA COVID-19 Funding and Reimbursements

The Conference of Mayors recently held the webinar "Maximizing FEMA Funding and Reimbursements Eight Months In," it is now available at no cost on-demand.

Eight months into the pandemic, many cities are preparing and submitting reimbursement requests to the Federal Emergency Management Agency (FEMA). This webinar provides useful information to assist cities in using available federal aid to respond to the impact of COVID-19 on cities and their residents.

Topics discussed are next steps and tips for recovery planning and the reimbursement process; required documentation and time table; updates on eligibility criteria for things like PPE, medically necessary resources, and safety equipment to avoid spread; important updates and issues from around the various FEMA regions; and a focus on city efforts.

(Source: U.S. Conference of Mayors)

Webinar: NG911 Roadmap Community Progress & Virtual Learning Tips

Join 911.gov on Tuesday, November 10, 2020, at noon Eastern for "NG911 Roadmap Community Progress and Virtual Learning Tips," a webinar on NG911 progress and distance learning needs. Registration is required.

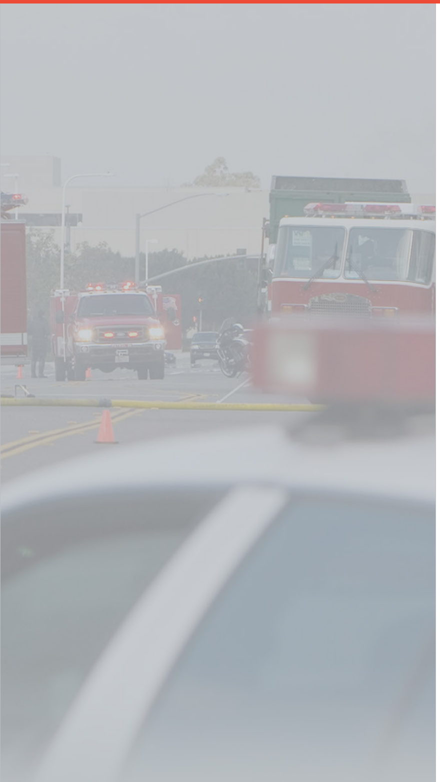
The NG911 Roadmap, released in 2019, outlines technical and non-technical tasks at a national level that must be completed to achieve a fully integrated NG911 system. A new easy-to-use tool, the NG911 Roadmap Progress Report, helps identify and track activities by organizations, associations and other groups in achieving those tasks.

This session will share how to use the tool, how to get involved and find out what it means for your organization. The success of NG911 is dependent on the 911 community's dedication and collaboration. Learn about the work underway and how you can champion your organization's involvement in this nationwide effort.

The second part, Adapting to Remote Learning and Training, discusses distance learning. Many jurisdictions and workplaces have struggled to meet current training needs during the pandemic. Discover tips and tricks to make remote learning and teaching just as effective as in-person courses.

See the 911.gov website for recordings of past State of 911 webinars and to sign up to receive emails about future offerings.

(Source: 911.gov)



Fair Use Notice:
This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

Disclaimer of Endorsement:
The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.

Cyber Threats

Can AI and connected tech foster better disaster decision-making?

Researchers at the University of Central Florida have launched a three-year interdisciplinary project to examine how artificial intelligence and smart technologies can improve collective decision-making among emergency managers, local government agencies, businesses and nonprofits. The goal is to reduce community vulnerability and enhance resilience.

Although smart technologies – like streetlights that monitor traffic flow or sensors that transmit real-time data about rising water levels – provide emergency managers with situational awareness, the increasing amount of data is becoming unmanageable without some AI assistance.

(Source: GCN)

Update: Ransomware Activity Targeting Healthcare and Public Health

CISA updated the advisory bulletin on ransomware targeting the Healthcare and Public Health (HPH) Sector, originally published October 28, 2020. Updates discuss specific threats being seen and rules of detection.

The advisory comes on the heels of attacks on dozens of hospitals while they attempt to meet demands of a spike in COVID-19 cases.

(Source: CISA)

How to improve cybersecurity for the workforce of the future

Cybercriminals love disasters for the opportunity to prey on citizens surfing the internet for information. COVID-19 is no exception. According to the FBI's Internet Crime Complaint Center, cyberattacks have roughly quadrupled since the pandemic began. The shift to remote working increased the number of possible failure points and created a large distracted workforce vulnerable to social engineering.

Cybersecurity leaders should prioritize, adopt and accelerate the execution of critical projects like zero trust, software-defined security, secure access service edge and identity and access management as well as automation to improve the security of remote users, devices and data. This paradigm shift will necessarily occur under tightening budgets and scarce resources, changing risk management and driving innovation in the field.

(Source: Search Security)

Malspam campaign milks election uncertainty

Threat actors have taken advantage of the uncertainty around the 2020 United States election to unleash a malspam campaign aimed at spreading the Qbot trojan. Criminals behind Qbot resurfaced the day after the election with a wave of spam emails that attempt to lure victims with messages claiming to have information about election interference, according to new researchers.

Qbot, an ever-evolving information-stealing trojan that's been around since 2008, reappeared this year after a hiatus to target customers of financial institutions with fresh capabilities to help it remain undetected. Its current incarnation has evolved into a "Swiss Army knife" of malware that can steal information, install ransomware, and making unauthorized banking transactions.

(Source: ThreatPost)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information